UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/619,912	07/19/2000	Julie H. King	RSW9-2000-0081-US1	1931

7590 07/12/2004

Jeanine S Ray-Yarletts
IBM Corporation T81 062
P O Box 12195
Research Triangle Park, NC 27709

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	**PAPER NUMBER**
2131	6

DATE MAILED: 07/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/619,912	KING ET AL.
	Examiner	Art Unit
	Michael R Vaughan	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-29 have been examined and are pending.

Response to Arguments

Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 5, 7-10, 14-17, 21-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Wood et al, hereinafter Wood (USP 6,609,198).

As per claims 1, 9, and 15, Wood teaches:

computer-readable program code means for enabling an identity change during a secure session using a digital certificate, further comprising (column 2, line 50 and column 9, line 56):

computer-readable program code means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof (column 12, lines 10-20),

computer-readable program code means for storing said digital certificate or a reference thereto at said server machine (column 13, lines 1-10);

computer-readable program code means for establishing a session from said server machine to a host system using a legacy host communication protocol, responsive to receiving, at said server machine, a first sign-on request from said client machine, wherein said first sign-on request identifies a first secure legacy host application to which said first sign-on is requested (column 5, lines 45-46 and column 9, line 27);

computer-readable program code means for passing said stored digital certificate or said reference from said server machine to a host access security system (column 9, lines 52-65);

computer-readable program code means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference (column 12, line 58—column 13, line 10);

computer-readable program code means for using said passed or retrieved digital certificate to locate access credentials for said user (column 13, lines 1-8);

computer-readable program code means for accessing a stored password or generating a password substitute representing said located credentials (column 13, lines 1-8);

computer-readable program code means, operable in said host access security system, for returning said stored password or generated password substitute to said server machine, along with a first user identifier corresponding to said located credentials (column 13, lines 5-8);

computer-readable program code means for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on, on behalf of said user of said client machine, to said first secure legacy host application executing at said host system (column 13, lines 10-25); and

computer-readable program code means for processing a second sign-on during said secure session using a second digital certificate for a second identity, further comprising (column 7, lines 59-60):

computer-readable program code means for receiving a second sign-on request at said server machine from said client machine wherein: (1) said second sign-on request identifies a second secure legacy host

application to which said second sign-on is requested; (2) said second sign-on requires authenticating a requester of said second sign-on; (3) said second secure legacy host application may be identical to said first secure legacy host application; and (4) said requester of said second sign-on is said user; (column 14, lines 34-52);

computer-readable program code means for retrieving said stored digital certificate or reference (column 13, lines 1-10)

computer-readable program code means for passing said second digital certificate or a retrieved certificate reference from said server machine to said host access security system (column 9, lines 52-65);

computer-readable program code means, operable in said host access security system, for re-authenticating said identity using said passed retrieved digital certificate or a retrieved reference which is retrieved using said retrieved certificate reference (column 14, lines 45-52);

computer-readable program code means, operable in said host access security system, for using said passed retrieved digital certificate or said retrieved reference to locate retrieved access credentials (column 12, line 60—column 13, line 10);

computer-readable program code means for accessing a retrieved stored password or generating a retrieved password substitute representing said retrieved credentials (column 13, lines 1-10);

computer-readable program code means, operable in said host access security system, for returning said re-accessed stored password or generated new password substitute to said server machine, along with said user identifier corresponding to said re-located credentials (column 13, line 10-12); and

computer-readable program code means for using said returned re-accessed stored password or new retrieved password substitute and said returned user identifier corresponding to said re-located credentials to transparently complete said second sign-on, on behalf of said requester to said secure legacy host application executing at said host system (column 14, lines 50-52).

As per claim 5, Wood teaches said communication protocol is a Virtual Terminal protocol (column 5, line 30).

As per claims 7, 13, and 19, Wood teaches said server machine is a application server machine (column 5, line 42).

As per claims 8, 14, and 20, Wood teaches computer-readable program code means for requesting by said legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user (column 10, lines 39-42 and column 14, lines 35-50);

computer-readable program code means for responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user (column 13, lines 26-44); and

said computer-readable program code means for using said returned password and said returned first user identifier to transparently complete said first sign-on further comprises:

computer-readable program code means for substituting said returned user identifier and said returned password or password substitute for said placeholders in said first sign-on message, thereby creating a revised first sign-on message (column 13, lines 1-12); and

computer-readable program code means for forwarding said revised first sing-on message from said server machine to said first secure legacy host application (column 13, lines 10-12).

As per claims 21, 27, and 28, Wood teaches computer-readable program code means for requesting by said second secure legacy host application, second sign-on information for said requester; and

computer-readable program code means for responding to said request for second sign-on information by sending a second sing-on message with placeholders from said client machine to said server machine, said placeholders

representing said user identification and said password of said user (column 13, lines 26-44); and

said computer-readable program code means for using said returned re-accessed password or new password substitute and said returned user identifier corresponding to said re-located credentials to transparently complete said second sign-on further comprises:

computer-readable program code means for substituting said returned user identifier corresponding to said re-located credentials and said returned re-accessed password or new password substitute for said placeholders in said second sign-on message, thereby creating a revised second sign-on message; and

computer-readable program code means for forwarding said revised second sign-on message from said server machine to said second secure legacy host application (column 14, lines 25-52).

As per claim 22, Wood teaches said second sing-on request includes information usable as proof that said second user owns said second digital certificate (column 12, lines 11-25).

As per claim 29, Wood teaches:

Establishing a secure session between a client and server using a digital certificate owned by a user of said client (column 2, line 50 and column 9, line 56);

remembering said digital certificate at said server (column 13, lines 1-10);

completing a first sign-on to a host application, by said server on behalf of said user, responsive to receiving an asynchronous sing-on request from said clients that identifies said host application, further comprising the steps of (column 5, lines 45-45 and column 9, line 27):

using said remembered digital certificate to authenticate said user to a host access security component (column 12, line 58—column 13, line 10);

if said user is authenticated, locating, by said host access security component, access credentials of said user (column 13, lines 1-10);

creating by said host access security component, a passticket that represents said located access credentials (column 13, lines 8-10);

returning said passticket from said host access security component to said server along with a user identifier associated with said located access credentials (column 13, lines 10-12); and

inserting said passticket and said user identifier into a log-on message in place of placeholders therefor, when said log-on message is received at said server from said client, thereby creating a revised log-on message that is then sent from said server to sign said user on to said host application (column 13, lines 26-44);

completing a second sign-on to a second host application, on behalf of user, responsive to receiving a second asynchronous sign-on request from said client that identifies said second host application, wherein said second host application may be identical to said host application (column 14, lines 34-52);

passing said remembered digital certificate from said server to said host access security component for authenticating said user for access to said second host application (column 9, lines 52-65);

if said user is authenticated for access to said second host application, location, by said host access security component, second access credentials of said user, wherein said second access credentials may be identical to said located access credentials (column 14, lines 45-52);

creating, by said host access security component, a second passticket that represents said located second access credentials of user (column 14, lines 49-50);

returning said second passticket from said host access security component to said server, along with a second user identifier associated with said second located access credentials (column 13, lines 10-12);

and inserting said returned second passticket and said returned second user identifier into a second log-on message that is then sent from said server to sign said user on to said second host application (column 14, lines 50-51).

Claim Rejections - 35 USC § 103

Claims 2, 10, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood in view of Carroll (USP 6,105,131).

As per claims 2, 10, and 16 Wood fails to teach that the certificates are x.509 certificates. Carroll teaches said digital certificate is an X.509 certificate and said digital certificate reference and second certificate reference are references to an X.509 certificate (column 6, line 11). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Carroll within the system of Wood because X.509 is a well-accepted standard of digital certificates, which uses proven security features.

Claims 3, 4, 11, and 17, are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood in view of Cohen et al (USP 6,178,511).

As per claims 3, 4, 11, and 17, Wood teaches a secure method of communication that utilizes legacy protocols (column 5, line 30). Wood does not explicitly teach the use of 3270 emulation protocol or the 5250 emulation protocol. Cohen et al teach the use of 3270 emulation protocol and the 5250 emulation protocol for a secure method of communication (column 4, line 27). Both the 3270 and 5250 emulation protocol are well established and known by those of ordinary skill in the art as a means to securely log a user into a system. Wood's method of communication is centered on security.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Cohen et al within the system of Wood because it would allow the system to securely logon a user

so that the user could then establish a secure connection with the other entities of the system.

Claims 23, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood in view of Nguyen (USP 5,689,566).

As per claim 23, Wood teaches that session IDs and objects uniquely identify the session between the client and server (column 11, lines 1-5). Wood does not explicitly teach that the session ID includes and random seed value concatenated with a sequence number. Nguyen teaches a second logon has a unique identifier, which includes a random number concatenated with a sequence number to provide a secure authentication protocol (column 4, lines 50-55). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Nguyen within the system of Wood because it would provide a more secure manner to transmit secretive information over an insecure transmission line. The use of random numbers and sequence numbers are well known in the art to defeat man-in-the-middle attacks because the random numbers or sequence numbers can be compared to all received numbers to stop a identical message from being resent.

As per claim 25, Wood teaches using an associated private key to encrypt the second digital certificate (Fig. 4).

Claims 6, 12, and 18, are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood and Cohen as applied to claims 3, 12, and 19 above, and further in view of Carroll.

As per claims 6, 12, and 18, Wood and Cohen fail to expressly teach that the host access security system, is Resource Access Control Facility system (column 2, lines 49-55 and column 3, lines 23-33). Carroll teaches the use of a host access security system is the function of a Resource Access Control Facility system (column 2, lines 49-55 and column 3, lines 23-33). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Carroll within the system of Wood and Cohen because a Resource Access Control Facility performs the same security functions as the security system of Wood to limit access to protected network resources.

Claims 24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood and Nguyen as applied to claim 23 above, and further in view of Schneier (Applied Cryptography).

As per claim 24, Wood and Nguyen are silent in expressly disclosing that the resource name is concatenated with the random seed value. The inclusion of the resource name adds further identifying data to the packet so that it cannot be replayed to another resource. Schneier teaches the authentication protocol,

Otway-Rees, whereby Alice, the client, generates a message consisting of a sequence number, a random number, and Bob, the resource being contacted, and encrypts all of these values so that only the authenticator, Trent, can read (page 59). This protocol would be advantageous for a client to reach a resource whereby the client must first be authenticated. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier with in the combined system of Wood and Nguyen because the log-on packet would also include the identity of the resource which makes the packet more unique and less susceptible to replay attacks.

As per claim 26, Wood teaches using an associated private key to encrypt the second digital certificate (Fig. 4).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael R Vaughan
Examiner
Art Unit 2131

MV

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100